[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/26
H04L 12/66

[12] 发明专利申请公开说明书

[21] 申请号 02116526.2

[43] 公开日 2003 年 4 月 16 日

[11] 公开号 CN 1411209A

[22] 申请日 2002.3.29 [21] 申请号 02116526.2

[71] 申请人 华为技术有限公司
地址 518057 广东省深圳市科技园科发路华为用服大厦
[72] 发明人 阮有明

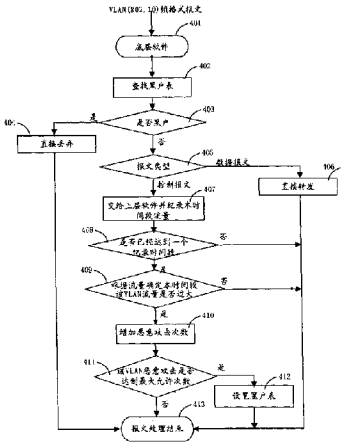
[74] 专利代理机构 北京德琦专利代理有限公司
代理人 王丽琴

权利要求书 2 页 说明书 8 页 附图 3 页

[54] 发明名称 一种检测并监控恶意用户主机攻击的方法

[57] 摘要

本发明涉及一种检测并监控恶意用户主机攻击的方法，解决宽带接入技术中的网络安全问题。针对采用虚拟局域网(VLAN)组网方案的以太网接入设备，通过检测 VLAN 下用户报文流量，达到防范恶意攻击的目的。包括：由支持 VLAN 的网络设备的底层软件，对来自设备网口的用户控制报文，先查找黑户信息表，判断其所属 VLAN 是否被记录在黑户信息表中；对于已被记录的用户，则直接丢弃其报文；对于未被记录的用户，则将其报文交给上层软件进一步处理并统计该用户所属 VLAN 下的用户报文流量；当某一 VLAN 下的用户报文流量多次超过设定值时，在黑户信息表中将该 VLAN 记录为黑户。黑户信息表，是以上网用户所在 VLAN 的标记(VLAN ID)作标识，对判断为恶意攻击的用户进行黑户信息记录。



ISSN1008-4274

1. 一种检测并监控恶意用户主机攻击的方法，其特征在于包括以下处理步骤：

A. 由支持虚拟局域网（VLAN）的网络设备的底层软件，对来自设备网口的用户报文，以报文所来自的虚拟局域网标记（VLAN ID）作索引查找黑户信息表；

B. 对于已被记录在黑户信息表中的上网用户，则直接丢弃其用户报文；

C. 对于未被记录在黑户信息表中的上网用户，进一步由上层软件进行处理并记录其所属VLAN的报文流量；

D. 当所记录的该VLAN下用户报文流量超过设定值时，在黑户信息表中将其所属虚拟局域网（VLAN）记录为黑户。

2. 根据权利要求1所述的一种检测并监控恶意用户主机攻击的方法，其特征在于：所述步骤A中的索引查找，是以加在上网用户主机报文以太网帧标签头上的虚拟局域网标记（VLAN ID）作索引项，以求摘要（Hash）方式查找所述的黑户信息表。

3. 根据权利要求1所述的一种检测并监控恶意用户主机攻击的方法，其特征在于：所述的用户报文是控制报文，支持虚拟局域网（VLAN）的网络设备的底层软件，对来自设备网口的数据报文，在对其控制报文判为合法时直接转发其数据报文。

4. 根据权利要求1所述的一种检测并监控恶意用户主机攻击的方法，其特征在于：所述的黑户信息表，是以上网用户所在虚拟局域网（VLAN）的虚拟局域网标记（VLAN ID）作标识，对判断为恶意攻击的用户进行黑户信息记录。

5. 根据权利要求4所述的一种检测并监控恶意用户主机攻击的方法，其特征在于：所述的黑户信息表，是以数组方式建立的，虚拟局域网标记（VLAN ID）为N的黑户，在表项中的位置为[N－N2]，$N2 \leqslant N \leqslant N1$，N、N1、N2为正整数。

6. 根据权利要求4所述的一种检测并监控恶意用户主机攻击的方法，其特征在于：所述的黑户信息表，是采取用固定内存作为表格存放地点的方式建立

的，虚拟局域网标记（VLAN ID）为N的黑户，在表项中的位置为：内存基址＋黑户信息表在设备内存空间中的相对起始地址＋[N－N2]×每个黑户的表项长度，N2≤N≤N1，N、N1、N2为正整数。

7. 根据权利要求1所述的一种检测并监控恶意用户主机攻击的方法，其特征在于：所述步骤D中的用户报文流量超过设定值，是连续记录到的一个虚拟局域网（VLAN）的用户报文超过一预定时间记录段。

8. 根据权利要求1所述的一种检测并监控恶意用户主机攻击的方法，其特征在于：所述步骤D中的用户报文流量超过设定值，是连续记录到的一个虚拟局域网（VLAN）的用户报文超过一预定的用户报文数。

9. 根据权利要求7或8所述的一种检测并监控恶意用户主机攻击的方法，其特征在于：所述的连续记录用户报文的流量是以用户的虚拟局域网标记（VLAN ID）为索引项建立流量信息表。

10. 根据权利要求1所述的一种检测并监控恶意用户主机攻击的方法，其特征在于：所述步骤D中将虚拟局域网（VLAN）记录为黑户，进一步包括：设置一恶意攻击次数Y，每记录到一次用户报文的流量超过设定值，则将恶意攻击次数记录增1，在记录的恶意攻击次数达到设置值Y时，在黑户信息表中将其虚拟局域网（VLAN）记录为黑户。

11. 根据权利要求10所述的一种检测并监控恶意用户主机攻击的方法，其特征在于：还包括设置一时间段，对于在该时间段内所记录的恶意攻击次数未达到设置值Y的虚拟局域网（VLAN），将已记录的恶意攻击次数清零。

一种检测并监控恶意用户主机攻击的方法

技术领域

本发明属于宽带通信技术领域，更确切地说是涉及一种通过检测虚拟局域网（VLAN）流量达到检测并监控用户主机恶意攻击的方法，可以应用于接入服务器、设备网关、路由器等宽带通信设备中。对本发明的描述，都以宽带技术领域以太网接入设备为例。

背景技术

随着互联网业务的迅速发展，上网用户数量越来越大，网络设备的稳定性和安全性日益成为网络规划的重要环节。

网络安全在宽带接入技术中一直是一个难以解决的问题。

图1示出一种典型的以太网接入宽带网络组网结构，上网用户主机接入Internet网，需经过支持VLAN的用户侧交换机〔LAN SWITCH〕、核心交换机、以太网接入设备和路由器。

上网用户主机通过支持VLAN的交换机连接以太网接入设备，在LAN SWITCH上进行适当的配置，使用户端发出的报文带有VLAN链路信息帧头，链路层格式符合802.1Q VLAN链路层协议。

对于宽带以太网接入设备，考虑到用户安全和管理的需要，一个VLAN所允许的用户数量是有限的，假设某宽带接入设备（VLAN接入业务）支持一个VLAN对应一个用户和一个VLAN对应多个用户两种方式。在一个VLAN对应多个用户的方式中，限制一个VLAN对应的最大用户数量为32个。

宽带接入设备（包括路由器、接入服务器等）的内部芯片一般采用网络处理器（NP），这类芯片的特点是转发能力极强，但处理能力较弱，这类芯片往往明显分为软件处理部分和报文转发部分。以Intel公司的IXP1200网络处理芯

片为例，它分为微引擎和Strong ARM Core两部分。其中微引擎主要负责报文转发，该部分的软件一般用汇编语言编写（微码），简练且效率极高，NP的转发性能主要来自于这个部分。而Core相当于一个普通的CPU，负责各种算法和报文处理工作，对于非直接转发的需要进行系列解析和算法处理的报文一般将由微码部分交给Core进行处理，该部分软件一般用高级语言来完成，算法复杂且庞大，所有通过网口进来的报文先要经过微码（底层软件）的处理后，然后分为转发报文和需要进行复杂处理的报文。对于转发报文一般处理较简单，将直接由微码转发出去；对于需要复杂处理的报文一般是微码无法处理的报文，将由微码把报文交给Core软件（上层软件）来处理。

用户一般使用两种报文上网，包括控制报文和数据报文。来自用户端的数据报文一般是用户的上网浏览报文，设备仅对其作简单处理后就直接转发出去，该过程不会对设备造成太大影响；但用户端的控制报文是用户上网的认证以及链路维护报文，在设备中需要经过上层软件复杂的流程和算法处理，以完成对上网用户的合法性和当前状态的验证和控制。

在众多网络攻击中，采用大流量报文进行攻击是恶意用户最常用的手段之一，尤其对于宽带网络，由于带宽非常大，当恶意用户通过一些网络工具、网络设备或者主机向接入设备频繁、大流量地发送控制报文时，势必给设备带来巨大负荷，接入设备软件底层与上层的通讯可能会成为瓶颈，CPU的处理负荷将会超载，从而影响正常用户上网流程的执行，造成其它用户无法上网，甚至发生因报文量太大而造成接入设备瘫痪。

发明内容

本发明的目的是设计一种检测并监控恶意用户主机攻击的方法，通过在接入设备网关上实现一种防止恶意攻击的保护网，使接入设备在收到恶意用户主机攻击时仍然能够正常工作，同时对恶意用户进行限制和采取相应惩罚措施。

实现本发明目的的技术方案是这样的：一种检测并监控恶意用户主机攻击的方法，其特征在于包括以下处理步骤：

A. 由支持虚拟局域网（VLAN）的网络设备的底层软件，对来自设备网口的用户报文，以报文所来自的虚拟局域网标记（VLAN ID）作索引查找黑户信息表；

B. 对于已被记录在黑户信息表中的上网用户，则直接丢弃其用户报文；

C. 对于未被记录在黑户信息表中的上网用户，进一步由上层软件进行处理并记录其所属VLAN的报文流量；

D. 当所记录的该VLAN下用户报文流量超过设定值时，在黑户信息表中将其所属虚拟局域网（VLAN）记录为黑户。

所述步骤A中的索引查找，是以加在上网用户主机报文以太网帧标签头上的虚拟局域网标记（VLAN ID）作索引项，以求摘要（Hash）方式查找所述的黑户信息表。

上述的用户报文是控制报文，支持虚拟局域网（VLAN）的网络设备的底层软件，对来自设备网口的数据报文，在对其控制报文判为合法时直接转发其数据报文。

所述的黑户信息表，是以上网用户所在虚拟局域网（VLAN）的虚拟局域网标记（VLAN ID）作标识，对判断为恶意攻击的用户进行黑户信息记录。

所述的黑户信息表，是以数组方式建立的，虚拟局域网标记（VLAN ID）为N的黑户，在表项中的位置为[N－N2]。

所述的黑户信息表，是采取用固定内存作为表格存放地点的方式建立的，虚拟局域网标记（VLAN ID）为N的黑户，在表项中的位置为：内存基址＋黑户信息表在设备内存空间中的相对起始地址＋[N－N2]×每个黑户的表项长度。

上述N、N1、N2均为正整数。

所述步骤D中的用户报文流量超过设定值，是连续记录到的一个虚拟局域网（VLAN）的用户报文超过一预定时间记录段。

所述步骤D中的用户报文流量超过设定值，是连续记录到的一个虚拟局域网（VLAN）的用户报文超过一预定的用户报文数。

所述的连续记录用户报文的流量是以用户的虚拟局域网标记（VLAN ID）为索引项建立流量信息表。

所述步骤D中将虚拟局域网（VLAN）记录为黑户，进一步包括：设置一恶意攻击次数Y，每记录到一次用户报文的流量超过设定值，则将恶意攻击次数记录增1，在记录的恶意攻击次数达到设置值Y时，在黑户信息表中将其虚拟局域网（VLAN）记录为黑户。

还包括设置一时间段，对于在该时间段内所记录的恶意攻击次数未达到设置值Y的虚拟局域网（VLAN），将已记录的恶意攻击次数清零。

本发明的方法是通过设计黑户信息表并根据某一特定时间段内VLAN流量，来监测和限制恶意用户攻击的。

在当今的以太网组网方案中，VLAN由于它的便于管理、安全性、减少广播等优点而被广泛采用，由于VLAN的区分一般是由通讯设备硬件来完成的，对于设计好的网络，VLAN对用户是透明的和不可改变的，所以本发明针对VLAN来设计网络安全防范措施，为采用VLAN组网方案的以太网接入设备提供了一个防范恶意攻击的行之有效的技术方案，可取得有益效果。

由于VLAN的实现一般是由网络设备（如：交换机）硬件实现的，而且以VLAN ID作为下标可以直接定位出黑户在设备内存空间的黑户表项区中的位置，所以本发明的通过检测某一VLAN的流量来监测和限制大流量报文恶意攻击的方法是可行且高效的。

附图说明

图 1 是典型的以太网接入宽带网络组网结构示意图；

图 2 是 802.1Q 协议标签头结构示意图；

图 3 是本发明的黑户在表项中位置计算方法示意图；

图 4 是本发明的接入设备底层软件对 VLAN 报文的处理流程框图。

具体实施方式

本发明采用连续纪录单个VLAN在一固定大小时间段内流量的方法，来检测用户是否存在恶意攻击的可能，即如果单个VLAN在某一固定时间段内的流量超过某一个界限，则认为该VLAN下的用户存在恶意攻击的可能，对于恶意攻击用户，采用纪录黑户表的方法来限制恶意用户的攻击和上网权限。

实施本发明方法时，需设计一张黑户信息表，用于纪录不合法用户或者对设备进行攻击的恶意用户的相关数据信息。接入设备的底层软件在接收到由设备网口接入的用户报文时，首先查找该黑户信息表，如果该用户在黑户信息表中已有记录，即已经被纪录为黑户，那么，不论该报文是什么类型、采用什么处理流程，底层软件都不对该用户报文作任何处理，而是直接丢弃。

该黑户信息表也可以记录那些认证没有通过的不合法用户的相关数据信息，从而可以对不合法用户的报文进行屏蔽，禁止其不断地向接入设备申请认证。此外，该黑户信息表还可对合法的但却曾经恶意攻击过接入设备的用户采取纪录并惩罚的措施。

参见图2，图中示出由802.1Q协议规定的标签头结构，由四个字节组成，前面两个字节Byte 1、Byte 2为标签协议标识(TPID--Tag Protocol Identifier)，它的值是8100，后面两个字节Byte 3、Byte 4为标签控制信息（TCI--Tag Control Information），标签控制信息的后12位是虚拟局域网标识(VLAN ID)，它唯一标识一个VLAN，共有$2^{12}=4096$个，值的范围为0～4095。

对于上网用户的身份可以以其所在VLAN的VLAN ID作为标识，由于VLAN标签头是由网络设备（一般是交换机）硬件加在报文以太网帧头中的，对用户是透明的和在物理上是不可更改的，所以以VLAN ID来标识用户是安全可靠的，同时由于VLAN ID是连续的数字，以VLAN ID作为下标来定位查找黑户信息表是可行而且高效的。

本发明的黑户信息表是以VLAN ID作为查找黑户的索引。

参见图3，图中示出查找黑户信息表、计算黑户在表项中的位置的方法。

对于某接入设备，假设该设备允许接入的最大用户数量为500，该设备配置的合法VLAN ID范围为500 – 999（N2 = 500，N1 = 999）。

如果以数组方式建立黑户信息表，如：UserList[500]，则对于VLAN ID为N（500=< N <=999）的用户表项位置为UserList[N - 500];

或者对于采取固定内存作为表格存放地点的建表方式，在最低地址至最高地址的设备内存空间中，则对于VLAN ID为N的用户表项位置（UserListLocation）为：UserListLocation = MemBaseAddr（内存基址，最低地址） + UserList_BeginAddr（表格的相对起始地址） + [N - 500] × ListLength（每个黑户的表项长度）。

参见图4，图中示出接入设备底层软件对VLAN报文的处理流程。

步骤401，接入设备的底层软件对接入的VLAN（802.1Q）帧格式报文进行处理;

步骤402，从报文中提取上网用户的VLAN ID，以VLAN ID为索引项，通过求摘要（Hash）的方式查找黑户信息表;

步骤403，判断黑户信息表中是否记录有该VLAN ID项，即判断该用户是否是黑户;

步骤404，如果黑户信息表中记录有该VLAN ID项，即判断该用户为黑户，即直接丢弃该用户的报文，然后执行步骤413;

步骤405，如果黑户信息表中没有该VLAN ID项的记录，即判断该用户不是黑户，并进一步执行步骤405;

步骤405，判断该报文的类型，是控制报文还是数据报文;

步骤406，若判断结果是数据报文，则直接转发该报文，转发完毕后执行步骤413;

步骤407，若步骤405的判断结果是控制报文，则进一步执行步骤407，进行VLAN流量检测，将控制报文交给接入设备的上层软件，并在本时间段内记录报文的流量。为了实时纪录用户控制报文的流量信息，接入设备底层软件保留对

每个用户控制报文的数据纪录，比如数组UserFlow[500]，VLAN流量表格也是以VLAN ID作为索引，采用如下步骤纪录某个VLAN的流量：

步骤408、409、410、411、412，通过判断是否已经达到一个记录时间段t的方法，来连续纪录每一个VLAN内用户在一个特定长度时间段t内的报文数量，或连续记录的一个VLAN内用户的报文数达到一定量，由于用户上网的控制报文一般很少，一个VLAN内对应的用户数量又是有限的，所以某一个VLAN在一个时间段内的控制报文数量应该是非常有限的，正常情况下的这个值与有恶意攻击时的报文数量相比较应该是微不足道的，所以可以决定在一个特定长度时间段t内，当一个VLAN的用户控制报文数量大于某一个设定值X时，可以有理由认为该VLAN下存在恶意用户，而可将该VLAN的恶意攻击次数记录或增加一次；如果当某一个VLAN的恶意攻击次数达到一个最大允许值Y时，则在黑户信息表中以VLAN ID为索引项记录该VLAN的黑户信息，如此，该VLAN的报文则会在下一次到达接入设备网口时就被底层软件直接抛弃，不会作任何处理（步骤403、404），而可以有效屏蔽掉恶意用户。

如果某一个VLAN在足够长的时间内没有达到最大攻击次数Y，那么可以将该VLAN的恶意攻击次数清零，这是为了防止将一些并非恶意的用户置成黑户，因为有些攻击可能是由于网络中的一些异常原因或者用户并非出于恶意而是由于操作不小心造成的。

对于一个VLAN对应多个用户主机（最多32个）的情况，当有一个用户主机被判断为恶意攻击用户从而造成VLAN被关闭时，网络管理人员利用现有技术会很快找到该恶意攻击用户，从而释放该VLAN，解决其它用户主机的上网。

本发明方法更适合的应用范围是将控制报文处理流程和数据报文处理流程分开，用户控制报文可以看作是用户状态和链路的维护报文，只有控制报文被设备认为是合法的，该用户才被认为是合法的，该用户的数据报文才能得到设备的直接转发处理。

本发明的技术方案经在相关设备上试应用，取得了预期的积极效果。

本发明的方法可应用于一切支持VLAN技术的网络硬件设备中，更适宜应用于需要对上网用户进行合法性认证处理的以太网接入设备中，对于不合法的攻击性用户报文可以直接丢弃，从而可以使设备免于被攻击。

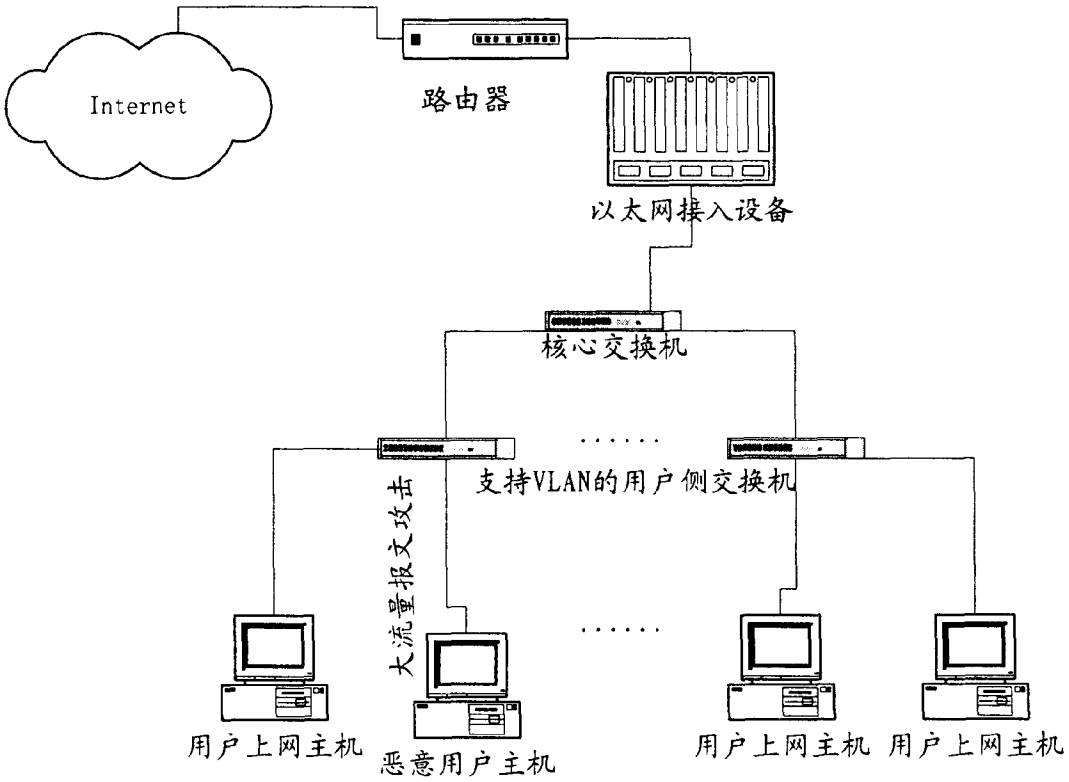

Internet
路由器
以太网接入设备
核心交换机
支持VLAN的用户侧交换机
大流量报文攻击
用户上网主机
恶意用户主机
用户上网主机
用户上网主机

图 1

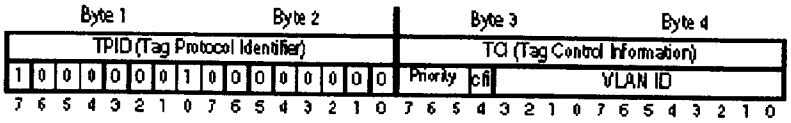

Byte 1
Byte 2
Byte 3
Byte 4
TPID (Tag Protocol Identifier)
TCI (Tag Control Information)
1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0
Priority
cfi
VLAN ID
7 6 5 4 3 2 1 0 7 6 5 4 3 2 1 0 7 6 5 4 3 2 1 0 7 6 5 4 3 2 1 0

图 2

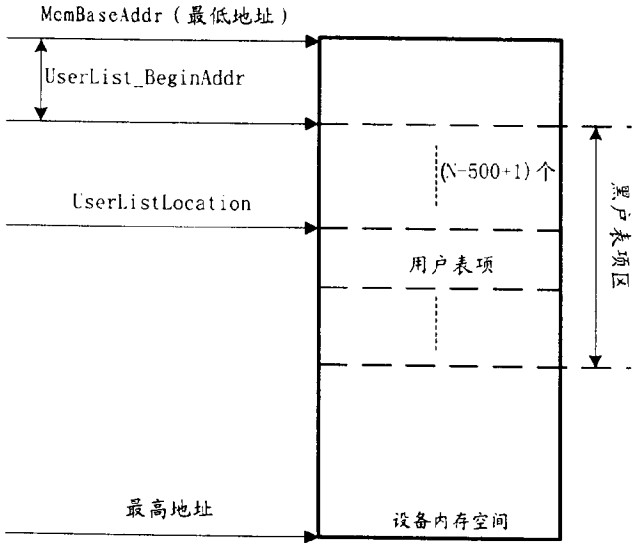

MemBaseAddr（最低地址）
UserList_BeginAddr
UserListLocation
(N-500+1)个
用户表项
黑户表项区
最高地址
设备内存空间

图 3

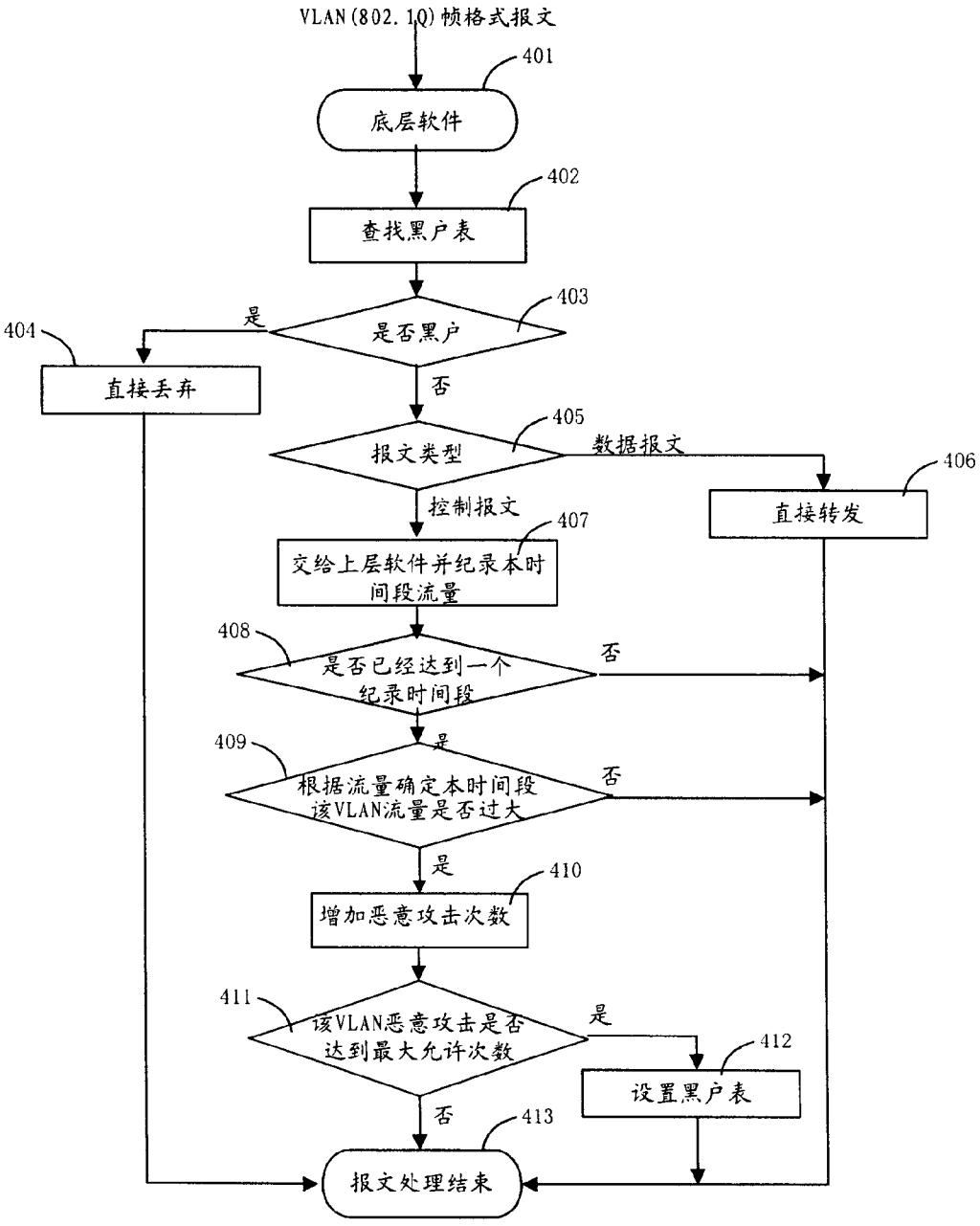

VLAN(802.1Q)帧格式报文
401
底层软件
402
查找黑户表
403
是否黑户
是
404
直接丢弃
否
405
报文类型
数据报文
406
直接转发
控制报文
407
交给上层软件并纪录本时间段流量
408
是否已经达到一个纪录时间段
否
是
409
根据流量确定本时间段该VLAN流量是否过大
否
是
410
增加恶意攻击次数
411
该VLAN恶意攻击是否达到最大允许次数
是
412
设置黑户表
否
413
报文处理结束

图 4